WHAT IS CLAIMED IS:

1. A method for communicating passwords comprises:

receiving at a server a challenge from a authentication server via a first secure communications channel, the challenge comprising at least a random password that is inactive;

communicating the challenge from the server to a client computer via a second secure communications channel;

receiving at the server a challenge response from the client computer via the second secure communications channel, the challenge response comprising a digital certificate and a digital signature, the digital certificate including a public key in an encrypted form, the digital signature being determined in response to at least a portion of the challenge and the private key; and

communicating the challenge response from the server to the authentication server via the first secure communications channel;

wherein the random password is activated when the authentication server verifies the challenge response.

2. The method of claim 1 wherein the client computer communicates the random password to a password-based security system, the password-based security system coupled to the authentication server.

3. The method of claim 2 wherein the password-based security system comprises a firewall.

4. The method of claim 1 wherein the public key and the private key are associated with an authenticated user.

5. The method of claim 1

wherein the private key is not associated with an authenticated user, and

wherein the authentication server does not authenticate the challenge response.

6. The method of claim 1 wherein the first secure communications channel is selected from the group: secure socket layer and secure HTTP.

7. A method for a client computer comprises:

receiving challenge data from a authentication server via a first secure communications channe, the challenge data comprising a challenge and a password that is inactive;

receiving a user PIN;

recovering a private key and a digital certificate in response to the user PIN;

sending the digital certificate to the authentication server via an external server, the digital certificate comprising a public key in an encrypted form;

sending a digital signature to the authentication server via the external server, the digital signature being determined in response the challenge and the private key; and thereafter

sending a user login and the password to a password-based security system coupled to the authentication server,

wherein when the authentication server verifies the digital signature, the password is activated.

8. The method of claim 7 wherein when the authentication server does not verify the digital signature, the password remains inactive.

9. The method of claim 7 wherein the password-based security system comprises a server selected from the group: a firewall and a VPN Gateway.

10. The method of claim 7 wherein recovering the private key and the digital certificate in response to the user PIN comprises:

recovering a private key associated with the user when the user PIN is correct; and

generating a private key not associated with the user when the user PIN is incorrect.

11. The method of claim 10 further comprising manually entering the user login and the password to the client computer.

12. The method of claim 7 wherein the password is activated for a pre-determined amount of time.

13. The method of claim 12 wherein after the pre-determined amount of time, the password is inactivated.

14. A method for a verification server comprises:

receiving a request for a one-time password from a client computer;

determining a one-time password, the one-time password being inactive;

communicating data comprising the one-time password to the client computer;

receiving user identification data from a user at the client computer;

verifying the user in response to the user identification data; and

activating the one-time password when the user is authenticated.

15. The method of claim 14 wherein communicating data comprising the one-time password to the client computer comprises communicating via an external server via a secure communications channel.

16. The method of claim 14 wherein the one-time password is selected form the group: random, pre-determined, pseudo-random.

17. The method of claim 14 wherein the user identification data comprises a digital signature.

18. The method of claim 17 wherein the digital signature comprises a private key selected from the group: associated with the user, not associated with the user.

19. The method of claim 18 wherein verifying the user comprises verifying the user when the private key is associated with the user.

20. The method of claim 14 further comprising:

receiving a verification request from a password-based security system, the verification request comprising a user login and the one-time password;

determining whether the one-time password is activated; and

approving the verification request when the one-time password is determined to be active.